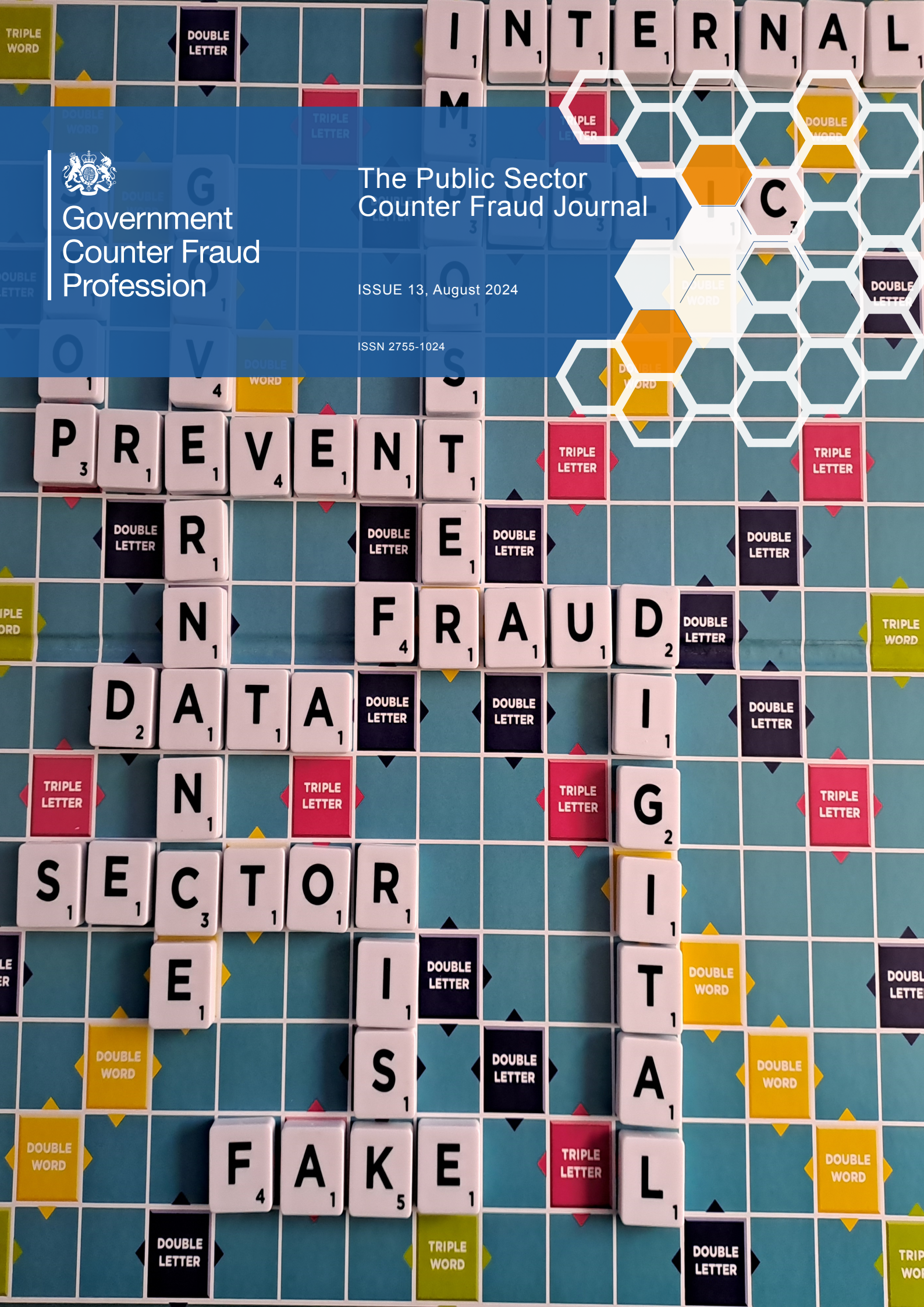


Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 13, August 2024

ISSN 2755-1024

Editorial Board

Toni Sless
Chair and Founder
Fraud Women's Network

Shawn Turner
GCFP Development Lead
Department for Work and Pensions

Professor Mark Button
Director of the Centre for Counter Fraud Studies

Laura Eshelby
Deputy Director,
Public Sector Fraud Authority

Mick Hayes
National Operations Manager,
NHS Counter Fraud Authority

Managing Editor: Cameron Massey
Cover Image: Parveen Akhtar








CONTENTS

Editor's Letter

This issues letter is provided by **Laura Eshelby**, the Chair of the Editorial Board. Laura is the Deputy Director of the Practice, Standards and Capability team within the Public Sector Fraud Authority (PSFA). She provides us her reflections as she prepares to depart from the PSFA.

Hello all and welcome to the 13th edition of the Public Sector Counter Fraud Journal. It's been 5 years since the first publication of the Journal which was published to align with the launch of the Profession. I hope you agree that as each edition comes out there has never been a shortage of engaging and interesting articles to enjoy.

This edition is no exception with articles from across a number of sectors, from passionate and expert individuals wishing to share their, in some cases, very personal reflections with you. Details of the articles you can enjoy are introduced for you below.

Before you read those though, I wanted to take this opportunity to formally step down from being the current Editor of the Journal, and my role in the Government Counter Fraud Profession. I will soon leave the PSFA to take on a new challenge, in a new sector.

I am still processing the fact that I am leaving what has been a dream role for me, being able to engage on a daily basis with like-minded, passionate and dedicated counter fraud practitioners - all striving to transform the way we reduce the harm caused by fraud, by building capability in those who lead the fight.

I came to this role in 2014, after a decade of investigating individuals and professionals alike, for alleged fraudulent activity in the Ministry of Justice. Being an investigator was the most exhilarating and exciting time for me, although stress inducing at times, particularly when my financial reports were being scrutinised by Judges and opposition counsel in court. I also remember having to literally leg it out of the back door following one confiscation hearing, tripping and cutting my leg - as I sought to escape from a rather angry family of a now convicted criminal who were not pleased 3 of their houses were being seized for sale to cover legal aid costs! Fun times.

I have spent much of the 10 years in the Cabinet Office and latterly the PSFA, helping to shape the Counter Fraud Function, and Government Counter Fraud (GCF) Profession.

My passion for the Profession

It's been the absolute privilege of my career to have the opportunity to help develop and grow the GCF Profession. Of course, all credit goes to the army of experts across sectors I have cajoled, threatened and begged to help me over the years. I'm eternally grateful for all your efforts and the time and energy put in from you all.

Another stand out moment of my career was formally launching the Profession in October 2018, with not one but 2 celebration events in London and Newcastle, and then being able to travel to New Zealand and Australia in quick succession to share our journey and approach with public sector and law enforcement colleagues there.

I also remember the angst and pain of developing each and every set of standards - they are never easy! And it's been brilliant to see how they have developed as products and how far and wide they are now used - even in Papua New Guinea, New Zealand and Australia! I am not exaggerating when I say that together we have achieved things that are world leading!

Since launch, 5 years ago, we have grown the Profession to 7,500 members - across 72 organisations. We have developed training in Risk and Measurement and launched the first bespoke Counter Fraud leadership academy for Functional Leaders.

A new Counter Fraud Handbook

Soon we will also have a new practitioner handbook, as the Blackstone's Counter Fraud Handbook is ready for publication. This was a way of myself and colleagues, David and Mike, giving back and sharing our knowledge from the build of the Profession. There's an excellent forword by our CEO Mark Cheeseman OBE, sharing his insights on how we counter fraud. We hope you will all support this and find it a helpful reference guide. All profits will be donated to Victim Support. (see pg.22)

https://www.amazon.co.uk/Blackstones-Counter-Fraud-Professionals-Handbook/dp/0198893027

My ask of you all

My ask is that as I move on to my next role you all carry on supporting and collaborating across sectors to ensure the ongoing development of the Counter Fraud Profession. So many of the articles we publish have this common theme - that we need to work together and across systems to have an impact - this is absolutely valid, and I implore you to act on this and play your part in whatever way you can to contribute to the efforts to understand, find and stop fraud.

As I sign off for one last time for the Profession, I want to reiterate my thanks to all of those I've had the pleasure of working alongside over the years. I would particularly like to thank Mark, our CEO, for believing in me, supporting me and being the ultimate architect and driving force for the GCF Profession.

Finally, I look forward to ongoing engagement in my new role with you all, which of course is still focussed on my area passion - how we counter fraud and economic crime.

Articles

In this edition we have an insightful article from Professor Yaniv Hanoch and Dr Stacy Wood who reflect on the need for a Cross system approach to tackling fraud. They explore the scale of fraud, now 40% of all crime in the UK is fraud related, and call for a new approach that holds financial institutions and businesses responsible for identifying or facilitating fraud. They conclude, in their view, that it's not reasonable to expect consumers to know when they're being defrauded and that responsibility should not be levelled at victims.

We have a great contribution from Sean McNabb, who is the Director for Cartel Enforcement, at the Competition and Markets Authority (CMA). He sets out the stark reasons that the CMA take bid rigging so seriously and the risks to look out for.

We then move on to a very personal piece from Lucy Cashin at Network Rail - offering a reflection of her career journey. Lucy recalls feeling lost, and subsequently falling into a counter fraud role and training to be an investigator. This is a story I have heard before about people falling into fraud roles and finding their calling, but Lucy tells her story in a truly compelling and honest way - I encourage you to read this one!

A return contribution from Cifas , with Rachael Tiffen, Director of Public Sector considering if anti-corruption training and awareness can influence meaningful counter-fraud change throughout local government? Rachael uses her experience and expertise of working with local government to explore this, and gives her views on what system and structural changes could tackle the issues identified.

Another really personal and authentic account, this time from reformed fraudster Alex Wood. There is always debate about giving air time to reformed criminals, but I personally believe the more we can understand the motivations of criminals the better we can consider the effective controls and steps we need as counter fraud officers to fight back. I thank Alex for his contribution and sharing his journey with us. A thought provoking reflection as Alex shares in his realisation that his fraudulent acts had been anything other than victimless.

Finally and by no means least, there is my interview with Becky Holmes. I had the pleasure of sitting down with Becky, author of the book 'Keanu is Not in Love with You'. We discuss the circumstances which led to her becoming involved in the world of romance fraud. We look at the perpetrators, the victims, as well as what more can be done to support and tackle this crime type.

Laura Eshelby, Deputy Director, Practice Standards & Capability, PSFA

We want to hear from you!

The Editorial Board are constantly looking for ways we can improve the Public Sector Counter Fraud Journal. You can help us by following the QR code below and completing the short survey.

https://www.smartsurvey.co.uk/s/gcfpjournal/

Get involved.

Would you like to be featured? Reach out to us at gcfp@cabinetoffice.gov.uk with your article suggestion.

To Tackle Fraud, we need a Multi-system Approach.

Have you or someone you know been a victim of fraud? If so, that's not unusual.

The UK's Office for National Statistics (ONS) reported a rise of 25%[1] in the number of fraud offences in 2021 compared to 2020 in the UK. Representing over 40% of all crimes against individuals, fraud is the most common crime[2] in the UK.

If these statistics are not alarming enough, there is some evidence that AI[3] is making it harder[4] to detect scams.

Author: Yaniv Hanoch, Professor of Decision Sciences, Center for Business in Society, University of Coventry

Author: Dr Stacey Wood, Professor of Psychology, Scripps College, University of Coventry

People often blame fraud victims[5] for being foolish or trusting enough to fall for a scam. But it's time to accept that it can happen to anyone. It's a problem so large we need to revise our concept of fraud as something that only happens to gullible or vulnerable people. The human brain can't keep up with all of the new technology-enabled types of fraud. We therefore need a new approach that holds financial institutions and businesses responsible for identifying or facilitating fraud and that harnesses AI to spot suspicious transactions. It's not reasonable to expect consumers to know when they're being scammed if banks and social media platforms can't.

Who falls prey to fraud?

If you were asked who is the most likely to become a victim of fraud, what would be your answer? If you are like most people, you probably thought about older adults[6]. Investment bankers, IT experts or young adults might not have come to mind.

This misconception about who is vulnerable or susceptible to fraud is one of the core problems surrounding the topic of fraud. For example, a 2010 survey[7] by credit reporting company Experian examining identity fraud in the UK found that two age groups, 25-34 and 35-44, represented 54% of the victims, while those over 65 represented only 4% of the victims of that type of fraud.

With cryptocurrency, victims tend to be young, well-educated, professional, and traders who have risky portfolios.[8]

It is enough to read the list of main investors (and victims) in the fraud-ridden cryptocurrency exchange FTX[9] and fraudulent medical technology company Theranos[10] cases to realise that even the savviest investors and celebrities can become victims. Their supporters included media moguls, politicians and hedge fund managers.

A 2023 report by UK Finance[11] indicates that 18 to 24 year-olds are being increasingly targeted by fraudsters, and are far more likely to fall prey to an impersonation scam, compared to those aged 65 and over. Also, the rate of 13 to 17 year-olds falling prey to scams via gaming[12] has seen a sharp rise.

1 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022
2 https://ukparliament.shorthandstories.com/breaking-fraud-chain-committee-report/index.html
3 https://www.forbes.com/sites/jeffkauflin/2023/09/18/how-ai-is-supercharging-financial-fraudand-making-it-harder-to-spot/
4 https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/
5 https://commsrisk.com/some-victims-of-fraud-are-just-stupid/
6 https://financialpost.com/executive/executive-summary/most-likely-financial-scam-victims
7 https://www.experian.co.uk/assets/insight-reports/brochures/The-Insight-Report-Victims-of-fraud-survey-March-2010.pdf
8 https://academic.oup.com/rof/article/26/4/855/6478303%20
9 https://markets.businessinsider.com/news/currencies/ftx-bankruptcy-top-investors-list-tom-brady-kevin-oleary-sbf-2023-1
10 https://www.integrityline.com/expertise/blog/elizabeth-holmes-theranos/
11 https://www.ukfinance.org.uk/news-and-insight/press-release/gen-z-more-likely-be-tricked-criminals-and-fall-impersonation-scams
12 https://www.lloydsbankinggroup.com/assets/pdfs/who-we-are/our-purpose/fraud/lloyds-bank-game-fraud-report.pdf

Developing educational and therapeutic programmes

Many schools around the world have introduced online safety programmes.[1]

The programmes currently on offer, however, tend to be rather thin on how to protect yourself from fraud. Children's charity the National Society for the Prevention of Cruelty to Children (NSPCC)[2], for example, has programmes for protecting children from online abuse, staying safe while using social media, and from legal but harmful content – but not for online scams.

Fraud prevention should be taught in schools and universities as part of the curriculum.

For older adults, charities such as the American Association of Retired Persons (AARP)[3] and AgeUK[4] offer guidance and resources, but it is unclear how effective or widely used they are.

Fraud prevention programmes, training, and information have rarely been scrutinised and we lack data on their effectiveness. We need to develop programmes for each age group and evaluate their effectiveness.

Improve deterrence

One of the most important theories in criminology is deterrence theory[5], which says crime reduction relates to the severity of the punishment, and, more importantly, the likelihood of being caught.

Research suggests[6] that increasing the likelihood of being caught is far more effective than increasing punishment. However, fraudsters have little to worry about. By the UK government's admittance[7] fraud accounts for over 40% of all crimes yet it receives less than 1% of police resources.

Businesses must better protect consumers

During the COVID pandemic, media outlets reported that Google blocked 18 million coronavirus scam[8] emails every day. Despite these efforts, according to a report[9] by the Federal Trade Commission (FTC), a US agency that enforces consumer rights, tech companies and especially social network sites are a breeding ground for scammers.

Indeed, the FTC reported that a quarter of the people who lost money to fraud said the process started on social networking platforms.

The nature of social media sites provides scammers with the ability to hide behind fake personas and pretend to be a legitimate business. They also allow scammers to reach millions of people with a press of a button - particularly younger adults[10] who tend to be more heavy and prolific users of social networking sites.

The FTC has issued orders[11] to a range of social media providers – including Meta, TikTok and YouTube – seeking information on how these companies screen for malicious and nefarious ads and scams.

Introduce new policies

California legislators are considering a bill[12] offering older adults greater protection against fraud by holding banks responsible when tellers facilitate fraudulent transactions.

In the UK, former home secretary Suella Braverman presented a fraud strategy[13] to the parliament in May 2023, which proposes a range of measures such as banning all phone calls related to financial products.

We see these two bills as a move in the right direction but more work is needed, and urgently. Policymakers must allocate funding to research and law enforcement agencies, introduce laws that provide greater protection to people, and collaborate with international law enforcement bodies, such as Interpol.

Fraud affects society on all levels: individuals, organisations and governments. We are all in it together, whether we like it or not.

1 https://educationhub.blog.gov.uk/2023/02/01/how-we-promote-and-teach-online-safety-in-schools/
2 https://www.nspcc.org.uk/keeping-children-safe/online-safety/?gclsrc=aw.ds&gad_source=1&gclid=CjwKCAiAg9urBhB_EiwAgw88mXcr3TpCRmIGbNM_A0C7uuvBV0uO6TrC4FpNSvyjP71aOIMRR4MM2hoCgPMQAvD_BwE&gclsrc=aw.ds
3 https://www.aarp.org/money/scams-fraud/about-fraud-watch-network/
4 https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/
5 https://www.house.mn.gov/hrd/pubs/deterrence.pdf
6 https://www.gov.scot/publications/works-reduce-crime-summary-evidence/pages/5/
7 https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public
8 https://www.bbc.co.uk/news/technology-52319093
9 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers
10 https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/
11 https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising
12 https://pluralpolicy.com/app/legislative-tracking/bill/details/state-ca-20232024-sb278/1277035
13 https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public

The Competition and Markets Authority headquarters, View Pictures/UIG/Getty Images via Bloomberg

Bid-rigging Risk in Public Sector Procurement:

why the Competition and Markets Authority Continues to take it Seriously

As someone who has made a career out of investigating bid-rigging in public sector procurement, I feel well placed to speak about the risks and consequences of such behaviour and why it continues to be an area of focus for the CMA.

Author: Sean McNabb, Director Cartel Enforcement, Competition and Markets Authority (CMA).

I began my career in cartel enforcement over 20 years ago at the Office of Fair Trading as an investigator and I am currently a Director in the CMA's Cartels Enforcement team. The CMA which was formed in 2014 when the OFT and the Competition Commission merged and is the UK's primary competition and consumer protection authority. Throughout my career, I've worked on many successful investigations across various sectors impacting public procurement spend, including leading the largest ever bid-rigging cartel investigation in 2009 that resulted in fines totalling £63.6 million issued to 103 construction firms found to have engaged in bid-rigging with competitors on building contracts, including many for the public sector.

More recently, I have been working on another significant case involving public sector contracts, this time in the demolition industry. The wrongdoing related to 19 contracts together worth over £150 million including contracts at the Metropolitan Police training centre, Bow Street Magistrates Court, and Coventry University. The firms colluded on prices when submitting bids. In addition, the CMA found that five of the firms, on at least one occasion each, were involved in arrangements by which the designated 'losers' of the contracts were set to be compensated by the winner. The value of this compensation varied but was higher than £500,000 in one instance. Some firms produced false invoices to hide this part of the illegal behaviour.

In my view, this latest case demonstrates that, despite the action the CMA has taken over many years against bid-rigging, there are some in industry not learning lessons from past wrongdoing. It's therefore vital that procurement officials are alert to bid-rigging risks, the the common red flags and what to do if suspicions are raised.

So, why is bid-rigging a priority for the CMA?

Bid-rigging is a form of procurement fraud, an anti-competitive arrangement between rival suppliers to undermine fair competition – on average it can increase prices by 20% or more.

Every year, billions of pounds are spent procuring goods and services in the UK. Where businesses compete to win contracts, purchasers get fair prices and choice, including more innovative products and services. However, when businesses engage in bid-rigging cartels, competition is undermined and customers can be ripped off, often spending more than necessary, and for less in return.

When it is the public sector that is the victim of bid-rigging activity, it is the taxpayer who loses out and that is why in the CMA 2024-25 Annual Plan we remain committed to clamping down on bid-rigging in public procurement that has a direct effect on public and household expenditure.

Actions the CMA is taking to uncover bid-rigging

At the CMA, we are always looking for new ways to generate leads and cases. We regularly present teach-ins on bid-rigging risk to public and private sector procurement officials, and we are seeing more cases coming through the pipeline as a result. To help public sector procurement teams deter and report bad practices we have a dedicated section on our website with helpful resources, including a free e-learning module designed specifically for the public sector and online training for local government officials in collaboration with the Ministry of Housing, Communities and Local Government.

New cartel screening tool

Another example of our proactive approach that I am particularly excited about is our work on cartel screening. In collaboration with international partners and the CMA's data science team, we are developing a screening tool called Bidviewer which we use to identify potential collusion between bidders through the analysis of tender data to identify suspicious bidding patterns.

We are looking to obtain further tender data to continue to test and develop the tool and are keen to work collaboratively with public sector bodies to test data patterns. If this is something that you would be interested in working with us on, please get in touch by emailing CMA_ ProcurementSupport@cma.gov.uk.

Powers of investigation

The CMA has strong powers of investigation which allow us to take action where we have reasonable grounds to suspect cartel activity and so, as the cases I've mentioned demonstrate, the risk to firms of getting caught is real. Our investigatory powers are wide ranging and include the ability to execute search warrants at both business and domestic premises and seize documentary and electronic material. We can also use a number of investigatory techniques such as conducting surveillance (including following and monitoring suspects and covertly recording conversations and meetings); use covert human intelligence sources (we can pay rewards to our informants of up to £250,000); and access communications data (for example, we can obtain mobile telephone records of individuals that we suspect to be involved in cartel activity).

How to reduce bid rigging risk

While the CMA has strong powers of investigation and will continue to come down hard on cartel behaviour where we find it, there are steps that those working in procurement can take to reduce their risk of falling victim to bid-rigging.

Firstly, be aware of what bid rigging is and what it looks like, as it can come in a variety of forms. Some of the most common bid-rigging strategies are:

Bid rotation
Companies agree to take it in turns to have the most attractive bid on a project, thereby ensuring that they all have an agreed share of the market;

Cover pricing
Companies that don't intend to win a contract communicate with their competitors and agree to submit inflated prices for the job so that another (often pre-arranged) bid from another company looks much better value;

Bid suppression
Companies agree to not submit a bid at all or to withdraw a previously submitted bid so that the designated winner's bid will be accepted.

These strategies are not mutually exclusive. For example, cover-bidding may be used in conjunction with a bid-rotation scheme. These strategies may also result in patterns that procurers can detect, and which can help them uncover bid-rigging schemes. This brings us to the second step that procurers can take to reduce the chances of them being a victim of bid-rigging, namely, to recognise the "red flags" that might indicate it is taking place.

Bid-rigging arrangements are difficult to detect because, as they are illegal, they are typically negotiated in secret. Therefore, it is vital to look for clues such as unusual bidding or pricing patterns. Certain bidding practices can seem at odds with a competitive market and unusual patterns in the way firms bid and the frequency with which they win or lose tenders can suggest bid-rigging is taking place. Some examples of common "red flags" include:

- The same supplier is often the lowest bidder
- There is a geographic allocation of winning tenders
- Some companies unexpectedly withdraw from the tender process
- Certain companies always submit bids but never win
- Bid prices drop upon the entry of a new or infrequent bidder
- The winning bidder sub-contracts work to unsuccessful bidders
- Tender documents submitted by different companies contain identical mistakes, such as spelling errors or miscalculations

This is not an exhaustive list and more details on the risk indicators (red flags) can be found on CMA website: Cheating or competing - Cheating or competing.

Finally, we recommend procurers design and manage their procurement process in a way that reduces the risk of bid-rigging and maximises the participation of genuinely competing bidders. Some steps we suggest to do this include:

- Avoid limiting the number of eligible bids
- Shop around when inviting bids
- Ask for bids to be broken down
- Avoid tender list management that incentivises firms to bid
- Keep records for comparison purposes
- Insist on a competitive process for sub-contracting
- Seek information on associated companies/subsidiaries
- Include warnings about competition law in tender documents
- Obtain signed declarations of non-collusion

Bid-rigging can occur in any sector, but there are some conditions that, in my experience, tend to make it more likely. These factors include:

- Where there is a limited number of suppliers
- Where the products and services being sold are similar
- Stable demand in the market
- Barriers to entry to the market
- Where an industry is facing difficult or uncertain times
- Where competing suppliers already know each other, perhaps via a trade association

The final point I want to make is that the CMA very much wants and encourages public procurers to report any suspicious behaviour to us. If you spot a "red flag" in a tender exercise, ask yourself whether this is what you were expecting or does it perhaps set some alarm bells ringing. Does the sector involved have any of the characteristics which might make bid-rigging more likely? Even if you are not sure, I would encourage you to speak to the CMA as it may be that we already hold some intelligence that links in with your suspicions. We do not expect fully evidenced complaints and with our strong powers of investigation, and the fact that bid-rigging in public procurement is a priority for the CMA, you can be sure that we will take your concerns seriously.

How to Report

If you've suspicions of bid-rigging, report it to the CMA.

Call the CMA on 020 3788 6888

Email: cartelshotline@cma.gov.uk

For more information visit: Cheating or competing - Cheating or competing

Succeeding in a Career in Investigation with a Disability

I had no idea what I wanted to do with my life. I went to an all-girls grammar school between 12 and 18 years old. I was shy, and most of the time, teachers would comment to my parents that I try hard. I did try, but the results for my A Levels were terrible. I received one A Level grade N (fail, a near miss) in Politics, One A-level grade E in Economics, and one AS-level grade E in computing. I had dropped a third A-Level as it was too challenging. Studying professional qualifications 30 years later, I better understand why I struggled. As an undiagnosed autistic child, I found learning environments overwhelming. My undiagnosed ADHD left me wanting to ask teachers questions, but being autistic made me so self-conscious and anxious that I didn't ask the questions. It took me longer to read exam questions as my mind would lose track, and I'd have to keep re-reading but still not "get" what they were asking. After leaving school, I worked in various admin and IT roles for a pharmaceutical company.

Auther: Lucy Cashin, Lead Investigator, Counter Fraud and Investigations Service Network Rail

After three years, the company offered to pay for me to study a specific degree (Business Information Systems). Instead of doing that, I handed in my notice and registered for a degree course in Software Systems for the Arts and Media. As a mature student at 25, the council funded my course fees. While studying full-time, I worked as a shop assistant for a retailer. I was diagnosed with ME (chronic fatigue syndrome) a year into my studies. Studying was an extra challenge, but I was determined to complete my degree. I graduated in 2006 with a BA(hons) 2:1.

When I graduated from university at 28, I felt elated when I was offered a graduate placement at an American business in the UK. My starting salary was much lower than my pre-degree salary at the pharmaceutical company. When I started the role, my energy was drained consistently. The company required employees to have natural hair colour and no visible tattoos. The working hours were 8 am to 6 pm, Monday to Friday and Saturday 8 am to 12 pm. I found the rules a bit strict, but I complied (no more bright hair colour!). They insisted we sign a form to opt out of the working time regulations. Alarm bells started ringing in my head, and I was told to make and receive calls even when driving. There was no provision for hands-free technology.

After a few months, I experienced painful and swollen knees and ankles. I could not drive a manual car anymore. Instead of supporting me, they treated me as a problem employee and did not offer any adjustments to my role. I was diagnosed with a type of arthritis. It was reactive arthritis, which meant my body reacted to viruses and attacked my joints. I handed in my notice without another job to go to. I had to attend an exit interview in a different location, and they even tried to give me a manual car to drive there. It was painful physically and emotionally. My manager was dismissed for gross misconduct due to my whistleblowing in my exit interview.

I felt lost and did not know what to do with my life. I registered with job agencies and was offered a six-month contract as a data analyst at a retailer. The role turned out to be a fraud investigation role, and I loved it! They were delighted with my progress and offered me a permanent role. With proceeds from the civil recovery for cases I had investigated, the business paid for the team to study a Bond Solon BTEC Level 7 Qualification – Advanced Professional Certificate in Investigative Practice. It gave me a greater understanding of investigative interviewing using the peace model and learning about laws such as PACE (Police and Criminal Evidence Act 1984) and RIPA (Regulation of Investigatory Powers Act).

I accepted a job in a different company. My role was as a data mining transaction analyst, and using the access I had to data, I assisted the police and other bodies (Department for Work and Pensions) by providing data in response to their requests. One of the cases I identified resulted in the conviction of a then-21-year-old who performed false refunds and false accounting to buy luxury holidays, gadgets and fast cars to a value of £85,000. He was sentenced to 18 months in prison.

I built up excellent relationships with different banks and helped with cross-border police investigations where suspected criminals were targeting shops in multiple police jurisdictions.

One of the employees I had investigated took the business to tribunal because they felt they had been unfairly targeted. I was called as a witness in the tribunal and wrote a witness statement explaining my investigation method. The lawyer told me it was one of the best witness

Within three months of being made redundant, I was offered the role at Network Rail as a Lead Forensic Technology Investigator within the Business Integrity Department. The business wanted to align with the terminology used by other arms-length bodies, so the department name changed to Counter-Fraud and Investigations Service, and my role became Counter-Fraud and Investigations Service, Lead Investigator.

I will celebrate my tenth year at Network Rail in August 2024.

Shortly after joining Network Rail, I gathered data about a potential fraud using a company credit card. It was a case that shocked people who worked with the fraudster. They had been a long-standing and well-respected employee. The level of deceit the person had gone to to carry out the fraud was immense. They had lied to family and friends, taking advantage of people's trust. The fraud amounted to almost £100k, and they made up a false story that a family member had been killed in an accident. They were dismissed and given a custodial sentence.

The year after I joined Network Rail, my mother became seriously ill and after a three-week battle, she passed away because of Pancreatic Cancer. My grief impacted my mental health, and it brought about challenges in my personal life. I was diagnosed as autistic in the year after she passed away. It helped me to understand myself better.

Over the past ten years, I've had the privilege of finding a vast, empowering network of disabled people. I joined the disabled employees' resource group called CanDo when it launched in September 2014. I've held various posts as a policy officer, chair, co-chair, and officer without portfolio. I've participated in incredible events and was invited to a royal garden party in 2018 to recognise my voluntary work supporting the disabled community at Network Rail. Highlights from my time in the network include holding a virtual event about women with ADHD that 275 people attended, arranging a private tour of Buckingham Palace for CanDo members, and being able to park within the Palace gates with my blue badge! I stepped down from the leadership team earlier this year, and I know that the CanDo team will continue to make positive changes for disabled people in the business.

I've raised awareness in the business regarding intersectionality. I created collaborative events that showcased intersectionality within the other employee networks. I arranged collaborations, including raising awareness of the charity Anthony Nolan and the need for more donors from minority ethnic backgrounds. I held an event with founder Sukhjeen Kaur from Chronically Brown, sharing her experience as a young, disabled woman of South Asian heritage. I held an online event with the Rt Hon Chloe Smith MP, and she shared her commitment to disabled people and championing the British Sign Language (BSL) Act in parliament. She reflected on her time as the minister for Disabled People, as well as her treatment for breast cancer.

I received a formal diagnosis of combined ADHD in February 2023. I've always felt like I have a chaotic brain. I often put objects down randomly and then forget about them. I struggle with "clear desk" policies in the workplace. Having support from colleagues (friends) who shared their experiences with me, and recommended books has helped immensely. My ADHD strengths include problem-solving, thinking and working creatively and uniquely. I am persistent and can hyper-focus on tasks and activities that I enjoy. I use noise-cancelling headphones while working (both at home and in the office) and have music playing to help me focus. I utilise the Do-Not-Disturb setting on teams when I need to concentrate without distractions.

I've worked in the counter-fraud field for the last sixteen years. I accidentally became a counter-fraud investigator, but I am glad I found this career path. It's never the same day twice. I see investigations as a challenge, almost a puzzle. I put the pieces together and either prove or disprove an allegation. Being autistic, I am an analytical and methodical thinker. I can focus and concentrate extensively and absorb and retain detailed information. I benefit from regular one-to-one meetings with my manager to review my priorities and ensure I know what is expected.

Over the years, I have learned to accept and understand my disabilities. I've learned about the social model of disability, which gave me the strength to say, "I am disabled!". The social model of disability is about removing the barriers that disable you, as opposed to the medical model that says your impairment or condition is the problem. Adjustments should be made to remove the barriers a disabled person faces, such as providing noise-cancelling headphones or the right equipment to work effectively instead. When I say I'm disabled, I am saying that I am disabled by the barriers in society. You are either disabled or non-disabled.

I worried that my disabilities would impact my working life. I now look at the positives. My life has progressed, and I've adapted to my disabilities. I gained new skills and persistence. I am a determined, tenacious person with a strong sense of justice. I have reasonable adjustments in place to support me, and by being supported, I am happy at work and want to do my best. If you treat disabled employees well, you will increase engagement and staff retention. Accessibility increases inclusion.

Can Anti-Corruption Training and Awareness Influence Meaningful Counter-Fraud Change throughout Local Government?

Having researched and drafted several English Local Government Strategies over the past 10 years as part of the Fighting Fraud and Corruption Locally (FFCL) Board, I read with interest the recent articles about corruption in local government.

Preventing corruption is a key part of good governance. It is linked to culture and behaviours, and detecting corruption is part of putting strategies into action and monitoring them. Overall, investigating corruption requires skills and unfettered access.

Author: Rachael Tiffen, CIFAS' Director of Public Sector

What does corruption look like and where can it happen?

Corruption can manifest in many forms in a local authority, and this may be contributing to a lack of specific data on these offences. From my own knowledge, some of the forms it can take are collusion, conflicts of interests, lobbying, cronyism, and bribery. There are areas of council activity which may be very susceptible to corruption, for example, planning decisions – called Section 106 agreements. These are agreements between a local authority and a developer for planning permission and to reduce a negative impact on an area that is being developed.

Corruption may be closely linked to bribery and there is guidance on the 'adequate procedures' that organisations should have in place to prevent it. The Bribery Act 2010 is also the legislation that

There is no legal definition of corruption but the most accepted one by Transparency International describes it as "the abuse of entrusted power for private gain". Prior to the Bribery Act 2010, the legislation covering this area were the Prevention of Corruption Act 1906 and the Public Bodies Corrupt Practices Act 1889. The common law offence of 'misconduct in a public office' still exists and has been in existence for over 100 years. In 2018 (the last available figures), there were 95 prosecutions.

The skills required to prevent and detect corruption

The ability to tackle corruption and its relationship to bribery is another factor to consider. However, to identify, assess, detect, and investigate bribery and corruption requires resource, skills, training and support by local law enforcement, for what may be a long and complex investigation.

Many local authority investigators are skilled and qualified and have developed counter-fraud strategies which lay out processes for reporting. Creating a culture to prevent, detect and follow through is essential and relies on a tone from the top.

Who has formal responsibility for the detection and monitoring of corruption in local authorities?

Prior to its abolition in 2015, the Audit Commission – the local authority regulator's counter-fraud team – produced a series of reports called 'Protecting the Public Purse'. Whilst not specifically focussing on corruption, its very existence shone a spotlight on counter-fraud activity. The National Fraud Authority (NFA), the penholders for the first Fighting Fraud Locally strategy, did not 'own' the strategy or activity but its work also focussed attention on local authority counter-fraud and corruption. The NFA was closed in 2013 and the local authority work was not transferred to any other body – which ultimately leaves a vacuum.

In recent times, Cifas has conducted an important piece of work – researching and drafting the last Fighting Fraud Corruption Locally (FFCL) strategy in 2020. 290 Councils attended 13 workshops to input into the counter-fraud and corruption strategy for local government, the FFCL 2020s – and there now being an active FFCL regional group across all English authorities who discuss risks – shows there is a vital commitment by counter-fraud practitioners to provide a co-ordinated response to fraud and corruption perpetrated against local authorities. Rather crucially too, the final section in the FFCL 2020s blueprint contains a checklist of activity for counter-fraud teams, and importantly, sections on what chief officers and elected members should be asking for, in order to get assurance that procedures are in place. Overall, the arrangements laid out in the FFCL 2020s strategy represent a holistic approach and should help to prevent corruption, if followed.

Tackling the insider threat

Nearly half (48%) of the 249 cases recorded to the Cifas Insider Threat Database between January-September 2023 related to dishonest conduct – a 35% increase compared to the same period in 2022. This emphasises the importance of staff feeling empowered to report dishonest conduct by colleagues before it escalates.

Whistleblowing is a crucial part of an anti-corruption programme and since incidents may be related to senior officers or local politicians, is it important that these programmes are appropriately resourced, complaints are treated as confidential, and are independent and recorded, as well as reported properly.

Internal procedures for the political governance of a local authority should have a framework including an audit committee, scrutiny committees and standards and ethics committees. However, these do not have responsibility for the physical operation of detecting or investigating. Additionally, whilst they have independent or lay members, they are mainly comprised of local elected members and officers of the council. Changing the culture means that these groups must be able to scrutinise and know what to look for – whole organisation fraud and corruption awareness is therefore essential.

The government delegation to 'armchair auditors' can be seen as part of a 'responsibilisation' strategy around transparency. But the elements of a responsibilisation strategy that covers self–governing tactics – such as due diligence and training – is not enough on its own. In isolation, no single strand can achieve a culture change. Additionally, the Nolan Principles cover the basis of the ethical standards expected of public office holders.

Individuals involved in local government corruption must be in a position to offer something and are typically in senior roles or, in some cases, at the very top of the organisation. So, the tone from the top is crucial and should reflect the 'adequate procedures' for preventing bribery and the culture strands of FFCL.

To conclude...

Corruption is by its nature difficult to uncover. Hidden and secretive, it takes specialist skills, the right mindset and training to expose.

Therefore, the business case for tackling corruption for a local authority must be weighted heavily on reputational risk, and doing the right thing morally and ethically. Reflecting on the example of T. Dan Smith, he faced a trial with negative publicity and ultimately served time.

If there is appetite, the incentive for tacking local corruption must be the ethical and moral one.

As local authorities are funded in part by central government grants for specific purposes, and by council tax and, in some cases, business rates revenue, the 'cost' of corruption may be passed on to the taxpayer. Since it will unlikely be budgeted for, this can be reflected in an increase of local taxes or taken from reserves, subsequently resulting in the reduction of critical services.

The argument internally for tackling corruption in this area should include the impact of corruption: where might the money go? What could it be funding? What are the global repercussions? Is it leading to trafficking? Does it undermine political democracy and fairness?

It is well known that fraud knows no boundaries geographically,

Additionally, with robust counter-fraud and corruption policies in place, there will be a stronger ability to monitor and report into the C-suite, to enforce meaningful change throughout. Training officers and locally elected members with general counter-fraud awareness whilst also providing the opportunity to obtain the skills needed to investigate, action, and record whistleblowing complaints in an unfettered way, can all help to strengthen a local authority team in a way that can influence an anti-fraud culture.

Today, awareness supported by the top table should focus on behaviour and culture change featuring ethical scenarios and perception surveys across the authorities. With the potential of having a single anti-corruption champion for local government linked to the FFCL initiative too, what might feel like a counter-fraud 'project' can soon transform into an 'honesty and integrity in local government programme'.

Interested in building your counter bribery and corruption knowledge? Find out more about the Cifas Fraud and Cyber Academy's Professional Certificate in Counter Bribery and Corruption and book onto our next course.

The Criminal Mind and the Future Threat of Generative AI

I am a reformed 'hyper-prolific' fraudster with dozens of convictions for dishonesty offences.

Author: Alex Wood, CEO of Reform Courses

I reached a major turning point in life when I discovered the extent to which my frauds had been anything other than victimless. One particular victim, upon realising that I had stolen £1.3M from his family-run company (and had not, in fact, been calling from his bank) suffered a stroke. The only reason that I had hitherto convinced myself that fraud was victimless was due to the very fleeting exchange that fraudsters have with their victims (especially with an Authorised Push Payment (APP) fraud) - most of my telephone calls lasted under an hour. Invariably, it is only when a fraud is detected and prosecuted that a perpetrator will learn of the devastation that he / she has wrought upon a victim.

Having spent some 8 of the past 15 years in and out of prison, I now work as a Keynote speaker and advise Senior Government, Police forces and global Tier 1 banks about fraud, money laundering, deep social engineering and the criminal mindset. I am leading the financial sector away from overreliance on the 'Fraud Triangle' as a means of understanding the fraud mindset and I help institutions to gain a deep insight into the criminal psyche.

I constantly reflect on my own journey into (and away from) criminality. I was not always a criminal - indeed, far from it.

As a child I was found to have a super-high IQ (something in the region of 170) and I was invited to join Mensa at 9 years old. I was a straight-A student, a chess expert and a violin prodigy. I turned down the offer of a King's Scholarship from Eton College in order to attend the Purcell School (a globally renowned specialist music school) and in my early teens I toured the world, performing the violin with internationally renowned orchestras and conductors. I became a regular at Buckingham Palace and Windsor Castle - the late HRH The Queen Mother funded my scholarship to attend the Royal College of Music.

My precocious talent was not simply attributable to my IQ. I was diagnosed with Aspergers when I was 15 - this accounted for my single-minded obsession to perfect my art through tens of thousands of hours of practice. But it also helps to explain my inability to properly cope with what happened next - when things went badly wrong.

In my early twenties, I developed repetitive strain injury (RSI) in my right wrist (my 'bowing' arm). This condition eventually caused my wrist to seize-up, rendering me unable to play. I was forced to cancel engagements at the last minute and became known as unreliable. The telephone eventually stopped ringing and my income ceased. Instead of retraining in another field, I fell into a deep depression and mourned the 20 years that I had spent training to perfect my art and memorise the entire violin repertoire.

I soon found myself unable to pay my mortgage and, faced with homelessness, I committed my first fraud - a crude scheme whereby I founded a company and sold a worthless share of it to friends of friends (people who still thought I was a successful man and who were unaware of my injury).

I transferred the proceeds of the fraud to my current account and paid my mortgage for the next few months. When the investors telephoned me for updates as to the performance of their investment, I ignored their calls. They reported me to the Police.

The fraud was so poorly executed that it took the City of London Police just a couple of days to unravel it. I pleaded guilty to 'Obtaining a Pecuniary Advantage by Deception' and was sentenced to three years in prison.

My first fraud can, absolutely, be understood by reference to the 'Fraud Triangle':

1) I was in a parlous financial situation ***("perceived pressure");***

2) I was able to dupe people into transferring me large sums of money by abusing their trust ***("perceived opportunity")***, and;

3) I was able to justify the fraud by saying "I would rather be in prison than homeless" ***("perceived rationalisation").***

Upon my release, I found it impossible to find a sustainable source of income or accommodation. I spent several years in and out of temporary jobs and endured several bouts of rough sleeping - all the while battling the effects of depression and neurodivergence.

Towards the end of 2014, I was regularly sleeping on a row

of seats in Terminal 5 of Heathrow Airport - it was warm, safe and I had access to charging points and shower facilities (I would sneak into the spa area of the Sofitel). In my holdall was a couple of changes of clothes (which I washed whenever I could) and my laptop, whilst in my pocket was four pound coins - the extent of my wealth.

One night, I sat in the public 'Departures' area, surrounded by weary travellers awaiting connecting flights. My usual row of seats was occupied, so I opened my laptop and browsed through the various booking websites, perusing the local 'backpacker' hostels where I might find a bed for the night. Sadly, the only available hostels were prohibitively expensive - starting at £8.00 per night (double the wealth in my pocket).

As I scrolled further down the list of establishments, the prices steadily climbed and the accommodation looked more and more inviting. I dragged the mouse to the very bottom of the page - Claridges hotel in Mayfair, with rooms starting at £800.00 per night.

I will not want to spoil the forthcoming Netflix docuseries, but I ended up spending the next 7 months living in every 5* hotel in Central London (including Claridges) without spending a single penny - by convincing them all that I was the 12th Duke of Marlborough. To my mother's horror, this campaign of offending made the national headlines.

Inevitably, the Metropolitan Police eventually caught up with me and I was sentenced to 3 ½ years in prison.

I spent the majority of this sentence at HMP Wandsworth where I was assessed as 'low-risk' (of involvement in drugs and violence) and duly sent to a wing with other white-collar offenders. I spent some 21 months with a fascinating array of financial offenders including several perpetrators of the LIBOR scandal, boiler room operators, fake solicitors, bent accountants and one chap who had stolen some £760 million from a large Irish bank and ended up owning buildings such as Lunar House in Croydon (which he rented out to the Home Office).

I would listen for hours on end to my fellow residents trading stories about the wealth they had accumulated, about the fast cars and jewellery they had bought, about how they had been apprehended and, inevitably, about how they planned to escape detection next time. Prison seemed to be something of a training environment - a place for criminals to regroup, network with others of a like-mind and prepare for further, more determined offending upon release.

After a few months, I was approached by the man who would eventually become my co-defendant. He had been imprisoned for his hand in a £113 million authorised push payment (APP) fraud. He seemed to know exactly how his Organised Crime Network had slipped up and was certain that he would not be caught next time. He told me that, with my posh accent and my quick mind, we would be able to steal many millions of pounds together. He teased me about the fact that my fraud had yielded zero cash whilst he had netted vast wealth - and yet, due to the tiered structure of the Sentencing Guidelines, his sentence was only a few months longer than mine. We were both due to be released in early 2017 and so we swapped numbers.

Despite the authorities being well aware that my fraud against the hotels had been born of homelessness, nothing was done to address this 'trigger' (priority for housing was given to those in physical or mental ill health) and I was released with £46.00 (the standard "discharge grant") and a sleeping bag. Having spent some 21 months in prison, I was in exactly the same situation as I had been prior to my arrest. The weather was foul and, for the very first time, I contemplated ending my life.

Instead, I called the number I had been given in prison.

That phone call marked the beginning of a criminal partnership which would last 9 months, devastate long-standing businesses, wreck lives and lead to us being sentenced to a combined 16 years in prison.

When I reflect upon this period of criminality, I recognise that I was presenting the majority of the traits of a "psychopath" (an informal term often used for a condition called antisocial personality disorder or ASPD), as set out on Dr. Hare's 'Psychopathy Checklist' including, but by no means limited to:

- Glibness / superficial charm
- Egocentricity / grandiose sense of self worth
- Proneness to boredom / low frustration tolerance
- Pathological lying and deception
- Conning / lack of sincerity
- Lack of remorse or guilt
- Lack of affect and emotional depth
- Callous / lack of empathy
- Parasitic lifestyle
- Short-tempered / poor behavioural controls
- Lack of realistic, long-term plans
- Impulsivity
- Irresponsible behaviour
- Failure to accept responsibility for own actions

And I can confidently assert that a large number of the other fraudsters described above shared the bulk of these traits also. Our premeditated, sophisticated, greedy, cold and ruthless criminality simply cannot be assessed by reference to the Fraud Triangle.

A significant portion of my work involves assessing emerging threats and using my insight so as to help financial institutions to inform their risk strategies by overlaying their counter-fraud algorithms with psychological indicators of the criminal mind (of the type briefly explored above) in order to help predict future attacks.

One pre-eminent emerging threat is Artificial Intelligence (AI).

The debate rages as to whether AI is a force for good or bad and, whilst I have yet to reach a final conclusion, I can write with confidence as to the ways in which AI will substantially bolster the toolkit of a 'bad actor' (which is no reference to Halle Berry in 'Catwoman' or to Mike Myers in 'The Love Guru'). Of course, 'bad actor' in this context refers to those who wish to attack the UK economy, whether lone fraudsters, organised crime networks (OCNs) or even nation states.

Firstly, it is important that one has a clear understanding of exactly what AI is. I rather like the definition published by IBM Research:

"Generative AI refers to deep-learning models that can generate high-quality text, images and other content based on the data they were trained on….. these models can take raw data - say, all of Wikipedia or the collected works of Rembrandt - and "learn" to generate statistically probable outputs when prompted".

One popular deep-learning model is, of course, ChatGPT by OpenAI. In recent days, Google unveiled their answer to ChatGPT, named 'Gemini'.

If we think about the anatomy of a typical APP fraud (whereby a fraudster contacts, say, a business and socially engineers an employee into making monetary transfers to mule accounts), models such as ChatGPT and Gemini can easily be trained to source potentially vulnerable companies and sectors. They could also be trained to create the 'perfect' script to be used to socially engineer the victim during the phone call - after all, such deep-learning models work on the basis of continuous improvement.

Another popular deep-learning model is Deepfake, which can be used to clone voices and video imagery. We have seen powerful examples of this in recent news, with sophisticated clones of Martin Lewis and Sadiq Khan making the headlines.

'Automated Fraud Device'

Using Deepfake, bad actors can create a 99% accurate clone of a voice with just a 3 minute sample of that person speaking. Voice samples are very easy to come across, for example, from corporate vlogs, training videos and online seminars.

A common 'malicious redirection' fraud involves a hacker 'scraping' the inbox of an Accounts Payable team at a business and then forwarding an authentic looking email requesting for the forthcoming invoice to be remitted in favour of different bank details. Fortunately, most businesses are wise to this type of fraud and will ignore the fraudulent request.

But imagine if, just a few moments after receiving the email, the accounts clerk receives a call from the Financial Director (from a trusted DDI or mobile number) stating that the change of bank details is, indeed, bona fide. Imagine that the clerk recognises the FD's voice and agrees to authorise the payment forthwith. Of course….. the FD's voice was a Deepfake clone and the trusted telephone number was spoofed.

And whilst a Deepfake clone sounds complex and expensive to create, there are many open-source websites enabling such activity (often for free).

If we consider future risk, it is inevitable that we will begin to see AI models being blended by bad actors in order to automate APP-style frauds from start to finish - a 'zero-touch' fraud, in effect, wherein each stage of the attack (from the identification of the victim, to the creation of a perfect script, to the delivery of the voice, to the sourcing of mule accounts and to the cashing-out of the proceeds) can be executed with very little human involvement.

Inevitably, this will give a single bad actor the ability to discharge multiple sophisticated attacks simultaneously, hitting thousands of victims concurrently. This is a frightening prospect indeed.

The automation of fraud is not a new phenomenon.

One of the men I met in HMP Wandsworth was Tony Coulston-Hayter, another career fraudster. Tony had created the machine (left) which enabled him to telephone the owners of cloned debit cards and replicate the IVR platform of their bank (in the case of this particular photograph, Barclays Bank PLC). The speaker system at the bottom of the image would play the real Barclays Telephone Banking prompts down the phone line whilst the red device at the top would detect and record the victim's PIN once the victim entered it on what he / she thought was the usual secure 'touchtone' line. Tony would then enter the victim's PIN into the PINSentry device and begin to authorise substantial online payments.

Tony was using this frightening machine 6 years ago. I have no doubt that you can all imagine the profound risks of this type of device being deployed alongside AI.

The general consensus amongst the counter-fraud community seems to be that AI will not, necessarily, lead to new genres of offence. It will simply enable existing modus operandi to be scaled and executed more successfully, with very limited human involvement (thereby slashing the risk of detection).

The good news is that Generative AI, whilst generating a substantial risk, also holds the answers. But only if the financial institutions and risk experts train AI models on precisely the correct data to enable them to take account of the ruthless criminal mindset. At present, bad actors are several steps ahead.

'Sad Keanu' , Vanity Fair 2019

A Conversation with Becky Holmes, Author of Keanu is not in Love with You: The Murky World of Online Romance Fraud.

The Public Sector Fraud Authority's Laura Eshelby sits down with Becky Holmes, author of the book 'Keanu Reeves is Not in Love With You: The Murky World of Online Romance Fraud". We discuss the circumstances which led her to becoming involved in the world of fraud and delve into her newfound area of expertise, Romance Fraud. We look at the perpetrators, and the victims, as well as what more can be done to support and tackle this crime.

What circumstances led you to become involved in the world of fraud?

I inadvertently got involved in the world of romance fraud through boredom during lockdown. I'd done everything that I possibly could to alleviate boredom, except join social media. So, as a last resort, I set up a Twitter account, purely to see what was going on in the world that wasn't on the COVID news agenda.

Laura Eshelby, Deputy Director, Practice Standards & Capability,

Becky Holmes - Author of Keanu Reeves is Not in Love With You: The Murkey World of Online Romance Fraud

Immediately I noticed that my inbox was full of these ridiculously good-looking young men telling me how great I was. I thought, I'm 45, I'm about four stone overweight, I've got ridiculous hair, and I really don't think I'm your type - they were all around 25, incredibly handsome and gym fit.

If it had been just one guy that had messaged me and said 'hello, you look lovely', I might have replied. But it was absolutely loads all at once - it was very obvious that something was amiss. Initially I blocked and deleted any approaches, but with it being lockdown I thought right, I'm going to reply and see what this is all about and whether I can waste some of their time.

All of the responses I received were much the same, very one-dimensional and predictable, so I started saying weirder and weirder things, just to see if I could get any form of reaction, but I got nothing. Absolutely nothing. They were just carrying on with a script. I started screenshotting my interactions and putting them up on Twitter. People really engaged with it.

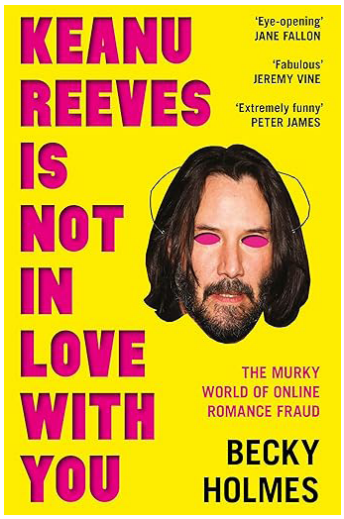
You have a sizable following on twitter (117k), do you feel as though your presence on the platform, and light hearted approach has created a space for victims to share experiences?

Definitely. People found the content I was posting really funny, but an unintended consequence of the growth of my account was that I started getting people privately messaging me saying that they had been a victim of romance fraud, and that nobody else in their life knew. I began speaking to people on the phone who'd been victims of romance fraud but didn't have anybody else to talk to. I'm not a counsellor and at that point I knew very little about romance fraud so I was just chatting to people, providing a listening and sympathetic ear. It quickly became apparent what a massive subject it is and also how misunderstood and under-reported it is.

Why do you think fraud is still so under-reported in the UK?

It's a complicated crime so I think there are many reasons, but there are two that I think top all others.

The first is that victims of romance fraud usually feel an incredible amount of shame after they discover that they have been defrauded. They think 'how could I have been so stupid?' or 'how am I ever going to live this down?' and it makes them hugely reluctant to come forward. The shame, embarrassment and guilt they feel is entirely needless - they have been the victim of a horrible crime - but the media usually treats victims of romance fraud with derision, which of course just makes other victims want to stay in the shadows.



Cover of 'Keanu Reeves is Not in Love With You: The Murky World of Online Romance Fraud

Secondly, a view that I share with a lot of people, is that what victims of romance fraud go through is very similar to what victims of domestic abuse go through. The fraudster, or abuser, uses coercive control to isolate the victim from their friends and family, they gaslight them into thinking they shouldn't be asking questions and they punish them with silence or threats if they don't do what they are asking.

I was in an abusive relationship years ago and friends had said to me, "What are you doing? Why don't you just leave him?". Victims of romance fraud get the same reaction. I know from personal experience that instead of agreeing with the person who is pointing out what is going on, you start defending the abuser or fraudster. This then means that the bond you have with the abuser or fraudster gets closer and you become increasingly isolated from the people around you.

If you're lucky, when you leave a relationship like this, people will embrace you and say, 'OK let's accept that this has happened - let me see how I can help you' and you will have a supportive network. However, sometimes people will say, 'Well, I told you so. What were you thinking? We've been through all of this. I told you this was going to happen.'

Language is really important- what do you think about the common use of the word scam - versus fraud, or crime?

In the book I talk about this issue a lot, with the main offenders being the media. One thing I am absolutely fed up with reading is how people 'fall for' scams. I hate that phrase. You wouldn't say, 'I fell for a burglary last night', or, 'I've just fallen for an assault', so when we say that somebody 'fell for' something, we are putting the onus on the victim and blaming them for having a crime committed against them.

What do you think is the worst thing about romance fraud?

The worst thing, by far, is the emotional distress. Of course, you lose money and that's very, very difficult and even shameful for many people. However, at the same time you also lose what you believe to be your future with someone you love.

If you've been talking to someone for a year to 18 months, and you've talked about getting married, your children, your dreams and you've shared links to houses you want to buy, you will feel like the relationship is very real and the future is bright. When it comes out as a fraud, it suddenly means you've lost the future that you've planned and that's very different to most types of fraud. And I think it's one of the things that's most misunderstood.

As humans, we want to be loved and we want to love. That will never, ever change and that is why romance fraud is potentially more dangerous than any other kind, because the human need for love will never change..

Is there a type of person (age, gender, etc) that is more likely to fall victim to romance fraud?

No. There is a stereotype of all victims being lonely middle-aged women, but I have spoken to people from 20 through to 75 years old, and from all walks of life, who have been targeted and ultimately defrauded. I've spoken to people currently out of work but also lawyers, CEOs and even a police detective. There is also a 50/50 split between men and women, although they are 'wooed' in very different ways.

What shocked you the most in your research?

To be honest, pretty much everything shocked me but I think it was the link to human trafficking I found the most eye-opening.

In Southeast Asia, as part of so-called 'pig butchering scams' there are people who are forced to commit fraud. That blew my mind. In China, during COVID people were losing their jobs and their incomes and couldn't survive. They started seeing adverts for organisations saying they were looking for people who were computer savvy, promising they could use their skills during

'Hundreds rescued from love scam centre in the Philippines', BBC News, 2024,

Can you elaborate on what 'pig butchering' is?

It's a cross between romance fraud and cryptocurrency fraud. Essentially what happens is that you will be wooed as you would be with the beginning of any traditional romance scam and the fraudster will earn your trust. The difference is that you won't be asked for money in the same way that romance fraudsters usually operate. However, at some point in the future, and it might even be a year down the line, they'll tell you that they've been making money on an investment platform.

You'll be persuaded to invest, seemingly be able to control your own investments through the platform and you'll even start to make money. You can put money in and you can take money out so it looks 100% legitimate. However, once you put in a large amount because you believe it's been going well, suddenly the platform goes down and your 'partner' disappears.

It's so clever because the people they're targeting are savvy investors, pretty much the opposite of the media's stereotypical romance fraud victim. The technology behind this kind of fraud is very intricate.

In terms of additional advice, are there any simple steps you would recommend people take to prevent this kind of fraud, or advice you can share to help anyone who finds themselves a victim of a romance fraudster?

This is a hard one because there is no dedicated, publicly funded support for victims of romance fraud. There are organisations and charities that people can go to, but they don't provide dedicated romance fraud support, and this type of fraud has a very different impact on people's lives because there's not only the financial impact, but the need for specialised emotional care as well.

A friend of mine, Anna Rowe, has teamed up with Cecile Fjellhoy, who starred in the Netflix-documentary "The Tinder Swindler". They've set up an organisation called LoveSaid (LoveSaid.org), a forum where people can ask questions and get advice. At this point in time LoveSaid.org is an organisation supported by volunteers with no dedicated funding, but they are extremely dedicated to raising the profile of romance fraud and have even spoken about it in the House of Commons. I personally would like to see LoveSaid.org receive government funding.

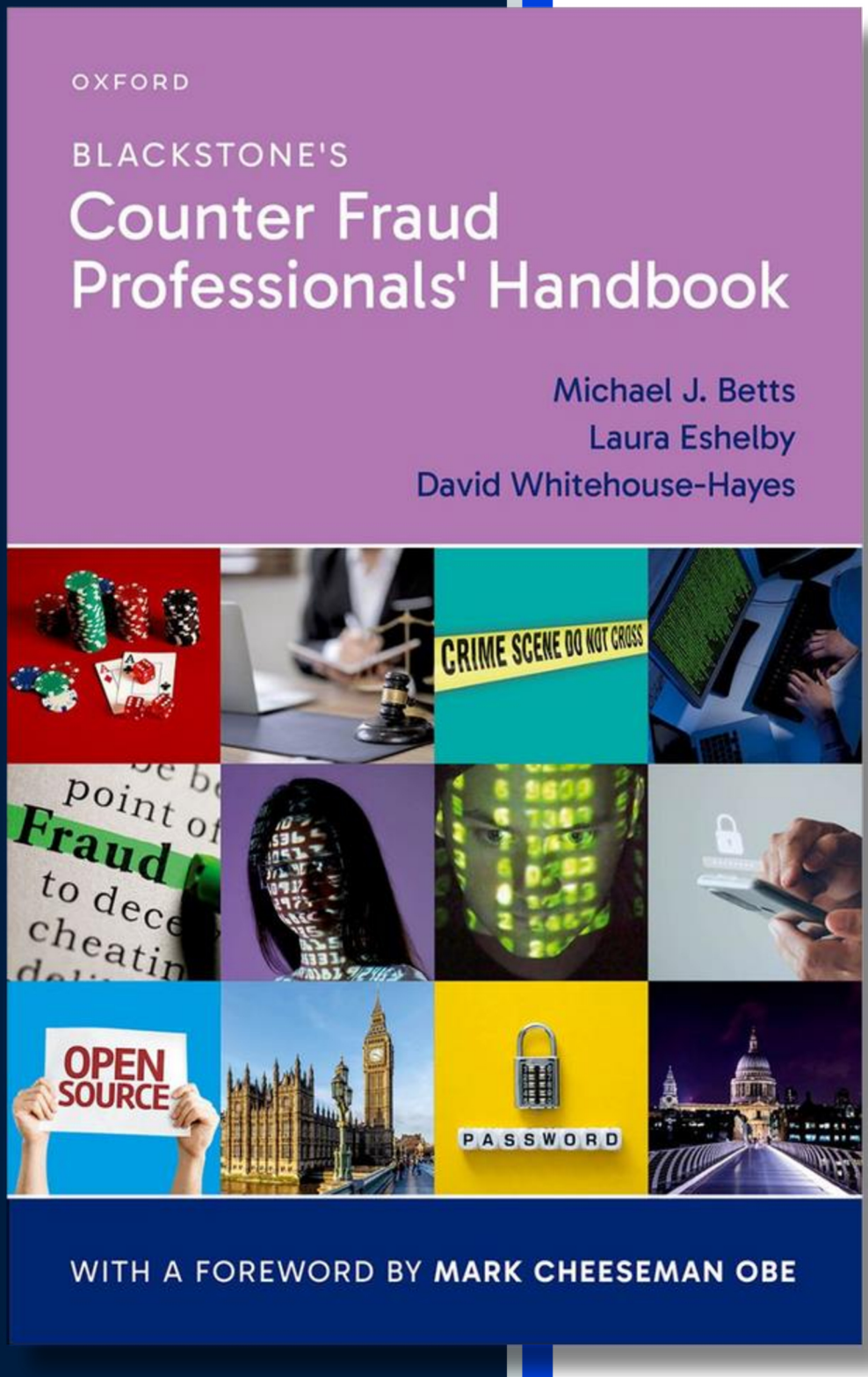
Romance fraud is psychologically harmful. People take time off work as a result and their mental health is seriously impacted. If you work in a bank or a building society and a romance fraudster asks you what you do for a living and you say I work in a bank, they think, bingo! So there's another way to get money which can affect corporations as well. It's much more far reaching than most people realise, and I think it needs to be acknowledged that it's not just a few women out there who've lost a bit of money. It's huge and there is no sign of it slowing down any time soon.

What one piece of advice would you give to people reading this who are worried about friends and family.

My advice to family and friends of anyone in this type of relationship would be to say to the potential victim, 'I'm not sure about this relationship. I know I don't know them like you do of course but I'm feeling a little bit worried about it'. Then you need to be very supportive and say to them that if anything does happen, you aren't going to judge them and that you will be here for them no matter what happens. You can also point them in the direction of organisations like LoveSaid, where they can go online and read at their leisure about the red flags and the potential dangers plus hear other peoples' stories.

As a friend or famizly member, you can't physically stop the relationship unless you're going to go to the extremes of taking away their devices, which I wouldn't advise. Most of the time, what you need to do is to get somebody thinking about the interaction and relationship, but not to the extent where they push you away. You need to make sure that you're there for them, if and when the worst happens.

OXFORD UNIVERSITY PRESS



Michael J. Betts,
Head of Capability and Learning, Public Sector Fraud Authority

Laura Eshelby,
Deputy Director, Public Sector Fraud Authority

David Whitehouse-Hayes,
Senior Manager, Public Sector Fraud Authority

September 2024
Paperback
9780198893028
312 pages

£39.99 (GBP)

Government
Counter Fraud
Profession

Contact us:

Email: gcfp@cabinetoffice.gov.uk
Web: https://www.gov.uk/government/groups/counter-fraud-standards-and-profession